**Technology Services Board Security Subcommittee Meeting Minutes**

## May 11, 2023 9:00 a.m. – 11:00 a.m. Attendees: Bill Kehoe, Cami Feek, Tracy Guerin, Sen. Joe Nguyen Hybrid – 1500 Jefferson St SE, Olympia, WA; Presentation Room and Virtual via Zoom

**Welcome, Agenda Review, 2/9/23 Minutes Review – Bill**

Bill Kehoe reviewed the agenda for the day and reviewed the Feb. 9 meeting minutes.

**Security Policy & Standard Review – Bill, Sam**

Bill reminded members these policies and standards were developed in a multi-agency, multi-discipline governance structure, where they have been reviewed and recommended for TSB approval.

* **Firewall Standard**:
  + Top of Form

Bottom of Form

updates include two basic criteria not currently required, but now added to the standard:

* maintaining the firewall rules within some form of a configuration management system, and
* showing through auditable records that each firewall change is reviewed by a qualified team of security professionals.
* **Media Sanitization and Disposal Standard**: updates include the new requirements for sanitizing media based on the type of data stored there and ensuring there is documentation.
* **Data Backup and Recovery Standard**: the key update requires agencies to test backups once a year and provides some additional resourcing and training to assist agencies.
* **Asset Management Policy**: this policy builds off existing processes, but closes a gap between the asset inventory and the evaluation of risks of operating those assets within the agency community.

Members reviewed the draft policies and standards, and recommended them for final approval at the June 8 full board meeting.

**Standard 112.10 – Technology Portfolio Foundation – Applications – Bill, Cammy**

Cammy Webster highlighted the business drivers behind this update including removing 46 questions as part of the state agency certification process and updated the core business functions to be more aligned with industry standards.

Members reviewed the draft standard, and recommended it for final approval at the June 8 full board meeting.

**Legislation – 2SSB 5518 – Concerning Cybersecurity – Bill**

Bill provided an update on recently passed legislation, effective June 23. The legislation introduces two significant components. The first is the establishment of the Cyber Security Advisory Committee as part of the Emergency Management Council within the military department. This subcommittee's focus is to strengthen security across critical infrastructure sectors like power grids and water systems. The committee's membership comprises representatives from local government, tribes, state agencies, higher education institutions, technology sectors, and first responders. The committee's key functions include assessing infrastructure risks, particularly cybersecurity risks, aligning with federal guidelines, and suggesting cyber incident response exercises.

The second component involves the Technology Services Board Security Subcommittee. It will now hold public meetings with provisions for closed sessions when necessary. Bill, as TSB Chair, will make additional appointments to ensure diverse representation, acknowledging that security concerns extend beyond experts. The subcommittee's activities encompass tabletop security exercises, data breach simulations, incident management, and policy review. The focus also involves analyzing incidents such as ransomware attacks to identify patterns and best practices for public agencies.

The legislation also requires an annual joint meeting between the Cyber Security Advisory Committee. This comprehensive legislation aims to enhance cybersecurity and response capabilities within critical sectors.

**State Local Government Cybersecurity Grant Program – Bill, Ralph**

Bill provided an update on the Cyber Security Grant program, highlighting significant progress made since the last update. This federal grant program, administered by CISA (a body under Homeland Security), allocates funds to Washington state over four years. The first-year allocation is around $3 million, with an emphasis on supporting local governments, particularly in rural and underserved areas.

A Cyber Security Planning Committee was formed to ensure compliance and effective distribution of funds. The committee, consisting of representatives from state agencies, local governments, and the health sector, has been meeting since November 2022 to develop the necessary cyber security plan. The notice of intent to apply for grants was sent out to local governments, resulting in an enthusiastic response with 60 completed notices already received.

The grant application is in its final stages of development and will be issued to local governments for formal application. The Statewide Cyber Security plan has also been developed and is currently undergoing final reviews before submission to the Federal Government for approval by June 30. The planning committee is also working on a thorough review process to score, rank, and select projects for funding.

**Current Threat Landscape - Ralph**

Not public information.

**State Security Operations Center (SOC) – Ralph**

Ralph Johnson introduced initial thoughts on the concept of a Strategic Threat Intelligence Center, a comprehensive approach to enhancing cybersecurity across various jurisdictions. He emphasized that this concept is not just a standard security operation center but aims to provide a range of services to local municipalities, particularly those with limited resources. The proposed center would offer 24/7 monitoring, automated incident response, threat and vulnerability management, and more.

Ralph outlined plans for forming a workgroup to define requirements and expectations. The center's structure would enable participation from various jurisdictions and be governed independently, ensuring affordability for even smaller entities. Further development is underway, and additional details will be shared in the future.

**Wrap Up – Bill**

Bill thanked the members for their engagement and adjourned the meeting at 10:15 a.m.